UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/817,543	03/26/2001	Stephen R. Hanna	SMY-246.01	6832

25181 7590 09/16/2004

FOLEY HOAG, LLP
PATENT GROUP, WORLD TRADE CENTER WEST
155 SEAPORT BLVD
BOSTON, MA 02110

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/817,543	HANNA, STEPHEN R.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-45 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-45 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 26 March 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 6/28/01 and 1/2/02.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-45 have been examined.

Claim Objections

2. Claim 19 is objected to because of the following informalities: "cryptographic processors" is duplicated (claim 19, p. 37, lines 20-21). Appropriate correction is required.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 38-40 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. It is not tangibly embodied as it is only a signal per se.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 19-22 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which

was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Claim 19 is directed to a method for communicating an ephemeral message involving four nodes and a tamper-resistant cryptographic processor. However, such a protocol is not described in the specification. There is no information as to what the role of the fourth node is and how it facilitates the communication of the ephemeral message. Thus, the disclosure fails to enable one skilled in the art to make and use the claimed invention. For examination purpose, it is interpreted that the first node and the fourth node are the same node. Claims that are not specifically addressed are rejected to by virtue of their dependencies.

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claim 41 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is not clear what corresponding structure for the means plus function to be found in the specification.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-9, 11, 17-30 and 35-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman (WO 01/20836 A2) in view of Spies et al. (6,055,314).

a. Regarding claim 1, which is representative of claim 35, 38 and 41, Perlman discloses a method comprising:

associating an expiration time with at least an ephemeral decryption key of an ephemeral key pair comprising said ephemeral decryption key and an ephemeral encryption key (fig. 1);

storing at least said ephemeral decryption key in a memory within a hardware device at a first node such that said ephemeral decryption key is not accessible external of said hardware device (p. 14, lines 7-15);

receiving at the first node an ephemeral message encrypted with said ephemeral encryption key (fig. 3, steps 44-46); and

decrypting said ephemeral message at the first node using said ephemeral decryption key to form a decrypted ephemeral message in the event the time said ephemeral message received and processed at the first node, which meets the limitation of a message time, is prior to said expiration time (p. 13, line 24 – p. 14, line 15).

Perlman does not disclose utilizing cryptographic functions such as key management (key generation, key storage and key destruction) and

encryption/decryption provided by a tamper-resistant cryptographic processor. Spies discloses utilizing cryptographic functions such as key management (key generation, key storage and key destruction) and encryption/decryption provided by a smart card, which meets the limitation of a tamper-resistant cryptographic processor, (col. 11, lines 26-57 and col. 12, lines 8-15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Spies smart card having cryptographic functions into the Perlman method. Accordingly, the smart card operates in conjunction with the first node. The motivation for doing so would have been that a smart card, a trusted device, could provide cryptographic capabilities without exposing them (col. 2, lines 35-44).

b. Regarding claims 2, 36 and 39, Perlman does not disclose the step of forwarding said decrypted ephemeral message to said first node. However, Perlman discloses that the first node is the intended recipient of the encrypted message (fig. 3, step 48); therefore, it is inherent in Perlman to forward the decrypted ephemeral message to the first node.

c. Regarding claims 3, 37 and 40, Perlman does not disclose the step of forwarding said decrypted ephemeral message to a second node. However, Perlman discloses that a second node is the intended recipient of the encrypted message (fig. 6, step 110) the second node receiving a decrypted ephemeral message from the first node, which is an ephemerizer (fig. 6, steps 106-108); therefore, it is it is inherent in Perlman to forward the decrypted ephemeral message to the second node.

d. Regarding claim 4, Perlman further discloses the step of generating said ephemeral key pair (fig. 3, steps 40-42).

e. Regarding claim 5, Perlman further discloses the claimed step of extinguishing at least said ephemeral decryption key (p. 14, lines 7-15).

f. Regarding claim 6, Perlman further discloses erasing at least said ephemeral decryption (p. 14, lines 7-15).

g. Regarding claim 7, Perlman further discloses that the extinguishing step comprises the step of preventing messages that are decrypted using said ephemeral decryption key from being forwarded outside of said tamper resistant cryptographic processor unit (p. 13, line 24 – p. 14, line 15).

h. Regarding claim 8, Perlman further discloses that the extinguishing step comprises the step of preventing messages that are encrypted using said encryption key from being decrypted using said ephemeral decryption key (p. 13, line 24 – p. 14, line 15).

i. Regarding claim 9, Perlman further discloses that key destruction capabilities are provided when the message time is subsequent to the expiration time and that key destroying includes erasing the ephemeral decryption key (p. 14, lines 4-15).

j. Regarding claim 11, Perlman does not disclose a timestamp accompanying said ephemeral message. However, Examiner takes Official Notice that having a timestamp accompanying a transmitted message to prevent replay attack is well known in the art. It would have been obvious at the time of the invention was made to have a timestamp accompanying a transmitted message since Examiner takes Official Notice that having

a timestamp accompanying a transmitted message to prevent replay attack is well known in the art.

k. Regarding claim 17, Perlman further discloses that the first node is coupled to a global communications network (p. 14, lines 26-30).

l. Regarding claim 18, Perlman does explicitly using a local area network. However, Examiner takes Official Notice that using a local area network within a small area is well known in the art. It would have been obvious at the time of the invention was made to one of ordinary skill in the art to use a local area network within a small area since Examiner takes Official Notice that using a local area network within a small area is well known in the art. Accordingly, the first node is coupled to the local area network.

m. Regarding claim 19, which is representative of claim 23, Perlman discloses a method comprising:

associating an expiration time with at least an ephemeral decryption key of an ephemeral key pair including said ephemeral decryption key and an ephemeral encryption key (fig. 1);

storing at least said ephemeral decryption key in a memory within a hardware device at a first node such that said ephemeral decryption key is not accessible external of said hardware device (p. 14, lines 7-15);

encrypting at a second node a message to form an encrypted ephemeral message, wherein said encrypting is performed using said ephemeral encryption key (fig. 6, step 104);

in a first transmitting step, transmitting said ephemeral message to a third node (fig. 6, step 104);

forwarding by said third node to said first node said encrypted ephemeral message (fig. 6, step 106);

decrypting said encrypted ephemeral message by said first node using said ephemeral decryption key in the event the time said ephemeral message received and processed at the first node, which meets the limitation of a message time, is prior to said expiration time (fig. 6, step 108);

in a second transmitting step, transmitting said decrypted ephemeral message from said first node to said third node (fig. 6, step 108).

Perlman does not disclose utilizing cryptographic functions such as key management (key generation, key storage and key destruction) and encryption/decryption provided by a tamper-resistant cryptographic processor. Spies discloses utilizing cryptographic functions such as key management (key generation, key storage and key destruction) and encryption/decryption provided by a smart card, which meets the limitation of a tamper-resistant cryptographic processor, (col. 11, lines 26-57 and col. 12, lines 8-15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Spies smart card having cryptographic functions into the Perlman method. Accordingly, the smart card operates to receive the ephemeral message for decryption from a node, the first node and output the decrypted ephemeral message to a fourth node, which is the same as the first node.

The motivation for doing so would have been that a smart card, a trusted device, could provide cryptographic capabilities without exposing them (col. 2, lines 35-44).

n. Claim 20 is rejected on the same basis as claim 19.

o. Regarding claims 21 and 25, Perlman further discloses the step of generating said ephemeral key pair (fig. 3, steps 40-42).

p. Regarding claim 22, Perlman further discloses the steps of encrypting said message at said second node with a third node encryption key having a corresponding third node decryption key held by said third node (fig. 6, step 104) and encrypting said message encrypted using said third node encryption key using said ephemeral encryption key to form said encrypted ephemeral message (fig. 6, step 104); and

following said second transmitting step, decrypting said decrypted ephemeral message using said third node decryption key to reproduce said message (fig. 6, step 110).

q. Regarding claim 24, Perlman further discloses that the first node is the intended recipient of the ephemeral message (fig. 3, step 48).

r. Regarding claim 26, Perlman further discloses extinguishing said ephemeral decryption key in response to a determination that said message time is subsequent to said expiration time (p. 14, lines 7-15).

s. Regarding claim 27, Perlman further discloses erasing said ephemeral decryption key in response to a determination that said message time is subsequent to said expiration time (p. 14, lines 7-15).

t. Regarding claim 28, Perlman further discloses preventing decrypted ephemeral messages from being forwarded to the second node in response to said determination that said message time is subsequent to said expiration time (p. 13, line 24 – p. 14, line 15).

u. Regarding claim 29, Perlman further discloses preventing said encrypted ephemeral message from being decrypted using said ephemeral decryption key in response to a determination that said message time is subsequent to said expiration time (p. 13, line 24 – p. 14, line 15).

v. Regarding claim 30, Perlman further discloses erasing said ephemeral decryption key in the event said message time is subsequent to said expiration time (p. 14, lines 7-15). Perlman does not disclose a timestamp included with the message. However, Examiner takes Official Notice that having a timestamp included with a transmitted message to prevent replay attack is well known in the art. It would have been obvious at the time of the invention was made to have a timestamp included with a transmitted message since Examiner takes Official Notice that having a timestamp included with a transmitted message to prevent replay attack is well known in the art. Accordingly, the timestamp is verified by the tamper resistant cryptographic processor to determined whether it is subsequent to said expiration time.

w. Claim 42 differs from claim 1 in that a timestamp associated with the ephemeral message is used in place of the message time. Perlman does not disclose a timestamp associated with the ephemeral message. However, Examiner takes Official Notice that having a timestamp associated with a transmitted message to prevent replay attack is

well known in the art. It would have been obvious at the time of the invention was made to have a timestamp associated with a transmitted message since Examiner takes Official Notice that having a timestamp associated with a transmitted message to prevent replay attack is well known in the art. Accordingly, the timestamp is used in place of the message time.

x. Regarding claims 43 and 45, Perlman discloses a method comprising:

associating a decryption lifetime with an ephemeral decryption key of an ephemeral key pair comprising said ephemeral decryption key and an ephemeral encryption key (fig. 1; p. 16, line 27 – p. 17, line 11);

storing said ephemeral decryption key in a memory within a hardware device at a first node such that said ephemeral decryption key is not accessible external of said hardware device (p. 14, lines 7-15);

extinguishing said ephemeral decryption key within said hardware device at the end of the decryption lifetime (p. 14, lines 7-15).

Perlman does not disclose the step of modifying said decryption lifetime such as decrementing an initial value periodically until an ending value is reached which is how a timer operates to keep track of and signal the end of time intervals. However, Examiner takes Official Notice that using a timer to keep track of and signal the end of time intervals is well known in the art. It would have been obvious at the time of the invention was made to use a timer to keep track of and signal the end of the decryption lifetime since Examiner takes Official Notice that using a timer to keep track of and signal the end of time intervals is well known in the art.

Perlman does not disclose utilizing cryptographic functions such as key management (key generation, key storage and key destruction) and encryption/decryption provided by a tamper-resistant cryptographic processor. Spies discloses utilizing cryptographic functions such as key management (key generation, key storage and key destruction) and encryption/decryption provided by a smart card, which meets the limitation of a tamper-resistant cryptographic processor, (col. 11, lines 26-57 and col. 12, lines 8-15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Spies smart card having cryptographic functions into the Perlman method. The motivation for doing so would have been that a smart card, a trusted device, could provide cryptographic capabilities without exposing them (col. 2, lines 35-44).

y. Regarding claim 44, Perlman further discloses receiving an ephemeral message encrypted with said ephemeral encryption key; and decrypting said ephemeral message in the event the current date is prior to said expiration date, which is equivalent to the event said decryption period has not reached said ending value (fig. 3, steps 46-50).

10. Claims 10, 12 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman and Spies as applied to claims 1 and 23 above, and further in view of Molva et al. (5,347,580). Perlman discloses generating the message time. Perlman also discloses that key destruction capabilities are provided when the message time is subsequent to the expiration time and that key destroying includes erasing the ephemeral decryption key (p. 14, lines 7-15). Perlman and Spies do not disclose that

the smart card includes an internal clock. Molva discloses a smart card including an internal clock (fig. 2). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Perlman and Spies such that that the smart card includes an internal clock, as taught by Molva, to generate timeliness indication and nonces (col. 3, lines 7-9). Accordingly, the message time is generated by the internal clock.

11. Claims 13-15 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman and Spies as applied to claims 1 and 23 above, and further in view of Menezes et al. ("Handbook of Applied Cryptography").

a. Regarding claims 13-15, Perlman and Spies do not disclose utilizing a trusted time authority to provide a timestamp for the message. Menezes discloses a method for providing timestamping service including the steps of sending a document to a timestamp agent, appending a timestamp to the submitted document and singing the composite document by the timestamp agent, returning the signed document including the timestamp to the submitter and verifying the timestamp agent's signature and thus verifying the timestamp (p. 581, see 13.8.1, Trusted timestamping service). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the method for providing timestamping service of Menezes into the combined method of Perlman and Spies, because the service is provided by a trusted third party.

b. Regarding claim 32, Perlman discloses that key destruction capabilities are provided when the message time is subsequent to the expiration time and that key destroying includes erasing the ephemeral decryption key (p. 14, lines 7-15). Perlman and Spies do not disclose that the message time is provided by a trusted time authority. Menezes discloses utilizing timestamping service provided by a timestamp agent (p. 581, see 13.8.1, Trusted timestamping service). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Perlman and Spies to utilize timestamping service provided by a timestamp agent, as taught by Menezes, because the agent is a trusted third party.

12. Claim 16 and 33-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman and Spies as applied to claims 1 and 23 above, and further in view of Silverbrook et al. (6,246,970). Perlman and Spies do not disclose erasing the ephemeral decryption key upon detection within the smart card of a predetermined condition indicative of an attempt to access at least said ephemeral decryption key. Silverbrook discloses erasing decryption keys stored within a smart card upon detection within the smart card of a predetermined condition indicative of an attempt to access said decryption keys (col. 3, line 64 – col. 4, line 24; col. 6, lines 18-25 and 58-64). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Perlman and Spies to include the step of erasing the decryption key upon detection within the smart card of a predetermined

condition indicative of an attempt to access said decryption key, as taught by Silverbrook, to deal with physical attacks on smart cards (col. 3, lines 58-61).

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Force et al. (5,533,123) discloses a Secured Processing Unit chip.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 703-306-5617. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

9/14/04

GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100